

concerning protection of privacy of individuals (see FAR Subpart 24.1).

239.7101 Definition.

Information assurance, as used in this subpart, means measures that protect and defend information, that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed, and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

239.7102 Policy and responsibilities.

239.7102-1 General.

(a) Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes, to include—

- (1) The National Security Act;
- (2) The Clinger-Cohen Act;
- (3) National Security Telecommunications and Information Systems Security Policy No. 11;
- (4) Federal Information Processing Standards;
- (5) DoD Directive 8500.1, Information Assurance;
- (6) DoD Instruction 8500.2, Information Assurance Implementation;
- (7) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management; and
- (8) DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.

(b) For all acquisitions, the requiring activity is responsible for providing to the contracting officer—

- (1) Statements of work, specifications, or statements of objectives that meet information assurance requirements as specified in paragraph (a) of this subsection;
- (2) Inspection and acceptance contract requirements; and
- (3) A determination as to whether the information technology requires protection against compromising emanations.

[69 FR 35534, June 25, 2004, as amended at 73 FR 1829, Jan. 10, 2008; 75 FR 34946, June 21, 2010]

239.7102-2 Compromising emanations—TEMPEST or other standard.

For acquisitions requiring information assurance against compromising emanations, the requiring activity is responsible for providing to the contracting officer—

- (a) The required protections, *i.e.*, an established National TEMPEST standard (*e.g.*, NACSEM 5100, NACSIM 5100A) or a standard used by other authority;
- (b) The required identification markings to include markings for TEMPEST or other standard, certified equipment (especially if to be reused);
- (c) Inspection and acceptance requirements addressing the validation of compliance with TEMPEST or other standards; and
- (d) A date through which the accreditation is considered current for purposes of the proposed contract.

239.7102-3 Information assurance contractor training and certification.

(a) For acquisitions that include information assurance functional services for DoD information systems, or that require any appropriately cleared contractor personnel to access a DoD information system to perform contract duties, the requiring activity is responsible for providing to the contracting officer—(1) A list of information assurance functional responsibilities for DoD information systems by category (*e.g.*, technical or management) and level (*e.g.*, computing environment, network environment, or enclave); and

(2) The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information assurance functional responsibilities.

(b) After contract award, the requiring activity is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked.

(c) The responsibilities specified in paragraphs (a) and (b) of this section